

Notice of Allowability	Application No.	Applicant(s)	
	09/487,946	JAKOBSSON ET AL.	
	Examiner	Art Unit	
	Jung W Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 09 August 2004.
2. ☒ The allowed claim(s) is/are 1,2,5-11 and 13-18.
3. ☒ The drawings filed on 19 January 2000 are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).**
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|---|--|
| 1. <input type="checkbox"/> Notice of References Cited (PTO-892) | 5. <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 6. <input type="checkbox"/> Interview Summary (PTO-413),
Paper No./Mail Date _____. |
| 3. <input type="checkbox"/> Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____ | 7. <input checked="" type="checkbox"/> Examiner's Amendment/Comment |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit
of Biological Material | 8. <input type="checkbox"/> Examiner's Statement of Reasons for Allowance |
| | 9. <input type="checkbox"/> Other _____. |

DETAILED ACTION

Response to Arguments

1. Applicant's arguments presented in the appeal brief filed August 9, 2004, specifically pg. 13, 1st paragraph, have been fully considered and are persuasive. The rejections of claims 1, 2, 5-11 and 13-18 have been withdrawn.

Allowable Subject Matter

2. Claims 1, 2, 5-11 and 13-18 are allowed.
3. The following is an examiner's statement of reasons for allowance: the independent claims of the instant invention define a method and apparatus comprising the steps of:
 - a. encrypting a data message m using a primary transmitter secret key z , known to the transmitter processor but not known to a receiver processor to form a quantity E ; and prepares a quadruplet (a, b, s, E) where:
 - i. $a = z * y^c \text{ modulo } p$;
 - ii. $b = g^c \text{ modulo } p$;
 - iii. $s = \text{signature } c(a, b, E)$
 - b. where $y = g^x \text{ modulo } p$, c is a random number, x is a receiver secret key of the receiver processor, and the parameters g , x and p are picked using a known encryption method; and

Art Unit: 2132

- c. wherein s is a signature, and wherein the transmitter processor determines s by using the same random number c that was used to determine a and b .
4. The independent claims further define a method wherein the quadruplet is transmitted from the transmitter processor to a receiver processor and comprising the steps of:
- d. verifying the signature s at the receiver processor;
 - e. decrypting a and b at the receiver processor by using the receiver secret key x to get the primary transmitter secret key z ;
 - f. using the primary transmitter secret key z to decrypt the quantity E and thereby obtaining the message m at the receiver processor.
5. The prior art of record cover a similar method and apparatus: specifically EKE with EL Gamal and digital signatures, but does not expressly teach using the same random number c to generate the signature c and to generate a and b .

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

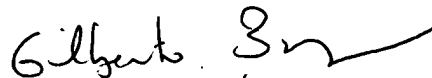
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Jung W Kim
Examiner
Art Unit 2132

Jk
February 25, 2005



GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100